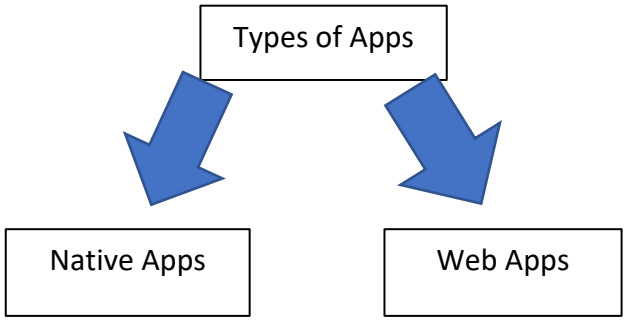
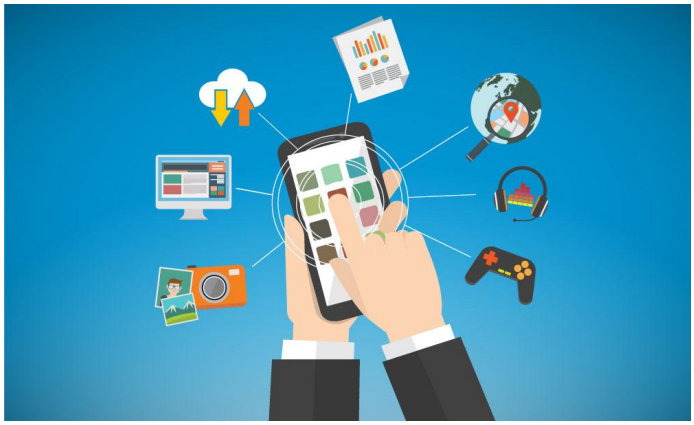
Mobile Application

Mobile Applications: Mobile application which is commonly called as an App, is a software that is designed to run on Mobile.
These are installed in the mobile through App Store (iPhone) and Play Store (Android) or inbuilt in smartphones which come with limited functionality like calculator, Weather, Chat, Mobile Web Browsing etc.



Native Apps: Native Apps are built for a specific mobile operating system (iOS or Android) they usually have better performance and more finely tuned UI.

Web Apps: Web apps are used in HTML5 or CSS and require minimum device memory since they're run through a browser. The user is redirected on a specific web page, and all information is saved on a server-based database. Web apps require a stable connection to be used.



Source: www.techopedia.com/
https://www.paymentsjournal.com/5-mobile-payment-security-concerns-to-consider/
https://blogs.quickheal.com/9-security-tips-using-mobile-payment-apps/

Activity 1: Guess the App

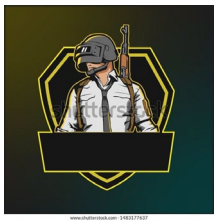
When: During the session
How: Guess the Mobile Applications based on the logos given below. Write the name of the application in the blank space.

_____

_____

_____

_____

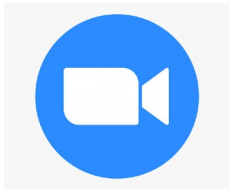


_____

_____

Source: www.techopedia.com/
https://www.paymentsjournal.com/5-mobile-payment-security-concerns-to-consider/
https://blogs.quickheal.com/9-security-tips-using-mobile-payment-apps/

_____



_____

_____

_____

_____

_____

Downloading apps in Android

Source: www.techopedia.com/
https://www.paymentsjournal.com/5-mobile-payment-security-concerns-to-consider/
https://blogs.quickheal.com/9-security-tips-using-mobile-payment-apps/

We find various kinds of Apps on the google play store of Android devices. First you have to go to the apps section of your smartphone. Open Google play store. Here you can search your app through multiple ways:

Via Search Icon
Tap on the magnifying glass and type the name of the app.
E.g. Search WhatsApp Messenger and now click go. You will get a list of matching apps. Few apps which are paid will reflect the price. Tap on the desired app and this will give you details about the app such as basic information, version, rating and reviews. You can decide whether to install the app or not based upon the reviews and ratings.

To Download the app, Click on Install. Then select "accept and download". Once installed select open to access the app.
For paid apps, you will have to make the payment first.

Via Keywords
Sometimes you don't know the name of an App. Then you can also search on the basis of keywords.

E.g. If you type messaging apps, you will get a list of relevant apps. Tap and download the desired app from the search results.

Via Categories
You can also search the app based upon the type and use of the app. Tap on Apps and then click categories. You'll get a list of categories like Heath & Fitness, Entertainment, Games etc. choose the category of your choice and get all the relevant apps. You can also use the further filter to segregate between paid and free apps.

Activity 2: Payment Apps

When: during session
How: Download and install any 1 mobile app that can be used to make online payment.
After you are done, write the steps you use here:-

_____
_____
_____
_____
_____
_____
_____
_____
_____

Source: www.techopedia.com/
https://www.paymentsjournal.com/5-mobile-payment-security-concerns-to-consider/
https://blogs.quickheal.com/9-security-tips-using-mobile-payment-apps/

Digital Security

Are mobile payments secure? This question emerged to every mind when online shopping and mobile payment came into the market. The flexibility and convenience levels it has come up with has made it trendier among the mobile users. The mobile payment options are rapidly replacing the outmoded payment options allowing the customers to make payments or complete transfer transactions through technologies like Android Pay, Samsung Pay, Apple Pay, Paytm wallets, and many more. However, when it comes to the security of making mobile payments, there are some loop falls.

5 Mobile Payment Security Concerns to Consider

1) Multiple Software Options

Similar to laptops and desktops, mobile phones are also working on various hardware and software systems. There are still some people who are using the old versions of iOS and Android globally. And this can lead to various security issues. The devices are not well supportive of the latest mobile security technologies which attract the hackers and fraudsters for exploiting and attacking.

Some of the examples of a secure mobile device include verification codes to mobiles or emails, face scanners, fingerprint scanner, geofencing, voice recognition, etc. Hence, look for a smartphone with advanced features regarding the software and hardware for an end to end protection of your payments and accounts.

2) Lost phone

Today, smartphones are similar to credit cards. It contains all the necessary details like the contact information, names, personal collection of photographs, social media connections, and whatnot. Similarly, it also provides complete access to bank accounts, debit cards, and credit cards through various payment apps, mobile wallets, online banking apps, and much more. But what if you misplace your phone at any store, restaurant, or any other crowded place? All your personal details are sure to get leaked right? And this includes all the banking and mobile payment details, which can lead to frauds.

Hence, it is better to look for smartphones that come with in-built protection to protect your phone, mobile phone wallets, and other fraud activities. Rather than looking for a single authentication method, go for a two-factor authentication process for unlocking the phone through facial recognition, fingerprint and iris scan options along with the PIN.

3) Inappropriate using habits

Source: www.techopedia.com/
https://www.paymentsjournal.com/5-mobile-payment-security-concerns-to-consider/
https://blogs.quickheal.com/9-security-tips-using-mobile-payment-apps/

Even if you have a highly secure mobile phone, the way you use your mobile phone can be problematic regarding payment security. Many mobile phone users use Google Chrome browsers for making payments through mobiles on Android phones. And browsers like Chrome and Safari are highly risky to use for making payments.
Look for secure and advanced mobile apps that come with an updated version. Lastly, there are mobile users who don't use any kind of PIN locks or other security options on their mobile phones, which allows the fraudsters to make frauds when the devices are lost. So, look for an updated payment app and browser for adding to the security of mobile phones.

4) Protect your mobile wallet

With the introduction of mobile payment options, several payment apps came into existence. Paytm, Google Pay, Apple Pay, PayPal, and many such payment wallets rapidly gained popularity with amazing offers, cashback, discounts, etc. All such applications work when a debit or credit card is added in the mobile wallet. Details like the card number, VCC number, expiry date of the card, etc. when entered in the application through encryption which is carried out through code. Again, the mobile wallet providers also use a token number generated randomly for making a payment which is not visible to the merchants while transactions are carried out.
The cybercriminals can misuse your account numbers, but when you add any credit or debit card to the payment apps using any public Wi-Fi, the risks increase to a great extent. The criminals can easily spoof off all the details used for making the transaction used while registering. For protecting yourself from such frauds, use your cards with mobile wallets while you are at home or having a personal network secured with a password. Using Virtual Private Network is also the best way to look for security while using a mobile wallet.

5) Beware of App Clones

Are you sure you have installed the right application on your mobile phone? Or is it one of the app clones? Such app clones come with ridiculous and poor security options that can be easily accessed by the criminals.

9 Security Tips

Source: www.techopedia.com/
https://www.paymentsjournal.com/5-mobile-payment-security-concerns-to-consider/
https://blogs.quickheal.com/9-security-tips-using-mobile-payment-apps/

#TIP 1 Download mobile payment apps only from official stores such as Google Play and Apple Store.

#TIP 2 Before you download any app, verify the publisher. The 'Top Developer' badge (in Google Play) is usually a good sign that the app is safe. Read its user reviews and just Google "Is (app name) safe?".

#TIP 3 Carefully read the permissions that the app asks for. If you think a mobile payment app is asking for more than what is required, do not install it. If you have any doubts regarding the permissions, just contact the app's manufacturer via their Twitter handle.

#TIP 4 Never visit an online banking or shopping website by clicking on a link received in an email or text message.

#TIP 5 Always choose a strong password for accounts for net banking or online payment apps. It should be a mix of uppercase and lowercase letters and special characters

#TIP 6 Do not use unsecured, public Wi-Fi networks for online banking or shopping. Doing so may let an attacker steal your information.

#TIP 7 Only use established and well-known websites for online shopping and paying for utilities.

#TIP 8 Ensure your banking transactions are OTP (one time password) enabled. While paying a purchase through net banking, debit/credit card, you will enter your login ID and password (or card details) and also an OTP (code sent to your registered mobile number) before you can make the final payment. So, even if an attacker manages to steal your net banking/card details, payment won't go through without the OTP.

#TIP 9 Install a mobile security app that is built with multiple layers of security. The Quick Heal Total Security App comes with SafePe besides other advanced features. SafePe is especially designed to secure your financial information when you use mobile payment apps for online shopping, banking, paying bills, etc.

Guess Me?

Source: www.techopedia.com/
https://www.paymentsjournal.com/5-mobile-payment-security-concerns-to-consider/
https://blogs.quickheal.com/9-security-tips-using-mobile-payment-apps/

1) I am a social networking app, a part of my name is also related to weight. Can you guess which APP I am?

a) Facebook
b) Instagram
c) Whatsapp
d) Truecaller

2) I am a famous E-Commerce app, where you will get all the products from A to Z. Can you tell who I am?

a) Myntra
b) Flipkart
c) Snapdeal
d) Amazon

3) I am a microblogging app, often used by politicians. I come with a word limit. Can you name me?

a) Telegram
b) Zomato
c) Twitter
d) Torrent

4) I am a professional networking app often used to build and engage your professional network. Can you guess who I am?

a) Naukri
b) Koo
c) Indeed
d) LinkedIn

5) I am an App to gain & share knowledge. People use my platform to ask questions and answer questions of various categories. Can you tell me my name?

a) Quora
b) Evernote
c) Coursera
d) Telegram[1]

Answer Explanation:

[1]Answer: 1-b, 2-d, 3-c, 4-d, 5-a

Source: www.techopedia.com/
https://www.paymentsjournal.com/5-mobile-payment-security-concerns-to-consider/
https://blogs.quickheal.com/9-security-tips-using-mobile-payment-apps/

1) The name in Instagram has “gram” , a unit of weight.
2) If you look at the logo of Amazon you’ll see an arrow originating from A and ending at Z. Which states that you will get all products from A to Z at Amazon.

3) Twitter is called a microblogging app as it comes with a word limit.
4) Although Naukri and Indeed are job portals, LinkedIn is considered as a professional networking social media.
5) Quora is a very interesting platform, where you can ask random questions and you can also answer the questions. It is also available in various regional languages.

Source: www.techopedia.com/
https://www.paymentsjournal.com/5-mobile-payment-security-concerns-to-consider/
https://blogs.quickheal.com/9-security-tips-using-mobile-payment-apps/